Gesicherte Unsicherheit

Jonas Botta 2019-12-24T10:59:00

Mit größter (An-)Spannung waren die am 19.12.2019 veröffentlichten Schlussanträge des Generalanwalts *Henrik Saugmandsgaard Øe* in der Rechtssache *Schrems II* erwartet worden (RS. C-311/18). Stehen doch in diesem Verfahren zwei tragende Säulen des internationalen bzw. transatlantischen Datenverkehrs zur Disposition: die Standarddatenschutzklauseln (kurz SCC) und der *EU-US Privacy Shield*. Eine erste Analyse der Schlussanträge legt gleichwohl nahe, dass auch zukünftig nur eines sicher ist: grenzüberschreitende Informationsübermittlungen bergen zahlreiche Unsicherheiten für die Betroffenen sowie die datenverarbeitenden Unternehmen.

Der Rechtsrahmen: Art. 44 ff. DSGVO

Dass der Geltungsanspruch der DSGVO weit über die Union hinausreicht, ist unter dem Schlagwort des „Marktortprinzips“ (Art. 3 Abs. 2 lit. a) bereits umfänglich diskutiert worden. Das besondere Zulässigkeitsregime für grenzüberschreitende Datenübermittlungen hat gleichwohl bislang weniger Aufmerksamkeit erhalten. Die in den Art. 44 ff. DSGVO niedergelegten Rechtsgrundlagen sollen gewährleisten, dass internationale Verarbeitungsprozesse das unionale Datenschutzniveau nicht untergraben (Art. 44 S. 2 DSGVO).

In der Praxis relevant sind insbesondere Durchführungsbeschlüsse der EU-Kommission, mit der sie das Datenschutzniveau in bestimmten Sektoren, Regionen oder ganzen Drittstaaten für mit dem Unionsrecht angemessen erklärt (Angemessenheitsbeschlüsse, Art. 45 DSGVO) und ebenfalls von der Kommission verabschiedete Klauselwerke, die zwischen einzelnen Vertragspartnern internationale Datenübermittlungen absichern können (SCC, Art. 46 Abs. 2 lit. c DSGVO).

Die Sorge: Das Ende des transatlantischen Datenverkehrs

Dass der EuGH nur vier Jahre nach seinem Urteil in der Rechtssache *Schrems I* (Rs. C-362/14) erneut über die Grundlagen des Datentransfers in die USA entscheiden muss, liegt darin begründet, dass das Ausgangsverfahren zwischen dem Datenschutzaktivisten *Max Schrems*, *Facebook* sowie dem irischen *Data Protection Commissioner* damals keineswegs sein Ende gefunden hatte.

Zwar hatte der EuGH 2015 geurteilt, dass das Safe-Harbor-Abkommen, der Vorgänger des Privacy Shield, kein angemessenes Datenschutzniveau gewährleiste. *Facebook Ireland* berief sich indes darauf, fortan SCC für den Datenverkehr an seinen Mutterkonzern *Facebook Inc.* zu nutzen. *Schrems* beantragte, diese

Vorgehensweise zu verbieten. Doch statt darüber zu entscheiden, verklagte die irische Datenschutzbehörde nunmehr ihn und das soziale Netzwerk, um über den *High Court* erneut ein Urteil des EuGH anzustreben. Dabei beschränkte sich das irische Gericht nicht darauf, die Rechtmäßigkeit der einschlägigen SCC (für Transfers zwischen einem EU-Verantwortlichen und einem Drittstaats-Auftragsverarbeiter, Beschluss 2010/87/EU) zu erfragen, sondern erstreckte sein Vorabentscheidungsersuchen auch auf den Privacy Shield. Der EuGH könnte mithin anders als noch vor vier Jahren beide Säulen des transatlantischen Datenverkehrs zeitgleich zu Fall bringen.

Der Ausweg: Die grundrechtskonforme Auslegung der SCC

Da SCC internationale Datentransfers in erster Linie ermöglichen sollen, wenn im Drittstaat kein angemessenes Datenschutzniveau vorherrscht (vgl. Art. 46 Abs. 1 DSGVO), hängt ihre Wirksamkeit insbesondere davon ab, ob sie die dortigen Defizite ausgleichen können.

Allein auf Grundlage des Wortlauts des Art. 46 DSGVO, der eben selbst keine Angemessenheit voraussetzt, ließe sich gleichwohl annehmen, dass die Anforderungen an die SCC niedriger als an die Beschlüsse gemäß Art. 45 Abs. 3 DSGVO seien. Zumal ein angemessenes Datenschutzniveau nach dem EuGH-Urteil zu *Schrems I* verlangt, dass „tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet [wird], das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist“ (dort, Rn. 73). Angemessenheit verlangt damit vielmehr Gleichwertigkeit und erfordert einen strengen Vergleich beider Rechtsordnungen.

Der Ansicht, dass der durch SCC gewährte Datenschutz sich als Minus zu den Angemessenheitsbeschlüssen erweise, tritt der Generalanwalt indes berechtigterweise entgegen (Rn. 115). Denn die Verwendung von SCC stellt den Verarbeitenden eben keine *Carte blanche* aus. Sie müssen auch tatsächlich einen entsprechenden Betroffenenschutz gewährleisten. Dies verlangt Art. 44 DSGVO von allen Rechtsgrundlagen, auch den SCC. Wesentlich dafür, ob die aktuellen (noch vor Geltung der DSGVO erlassenen) Klauselwerke diesem Anspruch gerecht werden, sind vor allem die Regelungen darüber, wann ein Datentransfer zu unterbleiben hat.

Hierbei vertritt der Generalanwalt eine grundrechtskonforme Auslegung der SCC. So sei nach Klausel 5 a) der Verantwortliche in der Union nicht nur dazu berechtigt, die Datenübermittlungen an den Auftragsverarbeiter im Drittstaat zu untersagen, wenn sich dieser nicht an die Klauseln halten kann, er sei hierzu auch verpflichtet (Rn. 132). Auf diese Weise lasse sich auch weiterhin vertreten, dass die SCC als zulässig anzusehen sind. Zudem bestimme sich ihre Wirksamkeit nicht allein nach den Pflichten für den Verantwortlichen, sondern auch nach den Befugnissen der mitgliedstaatlichen Datenschutz-Aufsichtsbehörden gemäß Art. 58 Abs. 2 DSGVO (Rn. 124). Denn wenn der Verantwortliche keinen ausreichenden Schutz gewährleisten könne, sei die zuständige Aufsichtsstelle in die Pflicht zu nehmen.

Der gescholtene Hüter: Der Data Protection Commissioner

Die Analyse des Generalanwalts zu den behördlichen Pflichten erweist sich als wahre Schelte für die irische Datenschutzbehörde. Weder schränke sie der Beschluss 2010/87/EU in ihren Befugnissen gegenüber *Facebook* ein – was die EU-Kommission bereits im Nachgang zu *Schrems I* klargestellt hatte (Beschluss [EU] 2016/2297) – noch verfüge sie im Rahmen ihrer Kompetenzen nach Art. 58 Abs. 2 lit. f und j DSGVO über ein so weitgehendes Ermessen, dass sie gar nicht handeln müsse (Rn. 144). Die Aufsichtsbehörde dürfe zwar darüber entscheiden, welche Maßnahme besser geeignet sei, aber sie müsse ihre Befugnisse zugleich vollumfänglich ausschöpfen (Rn. 148). Insofern nimmt der Generalanwalt der irischen Behörde zukünftig jeden Wind aus den Segeln, erneut voreilig auf Luxemburg zu warten, anstatt ihren Aufgaben ordnungsgemäß nachzukommen. In der Rechtssache *Schrems II* könnte damit weniger der transatlantische Datenverkehr und *Facebook* als vielmehr die „Hüter des Rechts auf Privatsphäre“ im Mittelpunkt des Urteils stehen.

Ein Folgeproblem aus der Inpflichtnahme der Aufsichtsstellen ergibt sich gleichwohl daraus, dass potenziell divergierende Einzelfallbewertungen ein einheitliches Kontrollniveau erschweren. Dies erkennt auch der Generalanwalt und verweist auf das System der interbehördlichen Kooperation (Rn. 155). Das Kohärenzverfahren i.S.d. Art. 63 ff. DSGVO ist indes kein Garant für schnelle Entscheidungen. Hier mag sich rächen, dass der internationale Datentransfer nicht im Zuständigkeitsbereich allein einer Datenschutzbehörde der Union liegt.

The Elephant in the Room: Der EU-US Privacy Shield

Ließe man es mit den Ausführungen des Generalanwalts zu den SCC bewenden, könnte man meinen, der große Paukenschlag sei in seinen Schlussanträgen ausgeblieben. Wäre da nicht der für den transatlantischen Datentransfer bedeutende Privacy Shield…

Zwar stehen SCC und Angemessenheitsbeschlüsse im System der Art. 44 ff. DSGVO gleichrangig nebeneinander. Insbesondere hindert die Existenz des Privacy Shield die Aufsichtsbehörden nicht daran, Datenübermittlungen, die auf SCC beruhen, zu untersagen. Dennoch ist das Bestehen eines (auch nur sektoralen) Angemessenheitsbeschlusses keineswegs folgenlos dafür, ob auf SCC gestützte Datentransfers in dasselbe Land zulässig sind.

Daher stellt auch der Generalanwalt zwar fest, dass sich der EuGH in der Sache *Schrems II* nicht mit dem Privacy Shield zu befassen brauche, führt hilfsweise aber dennoch zu dessen Rechtmäßigkeit vertieft aus (Rn. 187 ff.). Zumal der EuGH einer Entscheidung über den Angemessenheitsbeschluss nicht entrinnen kann. Sie steht

spätestens im Verfahren der Nichtregierungsorganisation *La Quadrature du Net* gegen die EU-Kommission an (Rs. T-738/16).

Ob der Privacy Shield ein angemessenes im Sinne eines gleichwertigen Datenschutzniveaus zu gewährleisten vermag, ist anhand eines umfassenden Rechtsvergleichs zu ermitteln. Die dadurch gewonnenen Einblicke in das US-Rechtsregime, vornehmlich in die Zugriffsrechte dortiger Sicherheitsbehörden, strahlen auch auf die Zulässigkeit von SCC aus, die Datenübermittlungen über den großen Teich rechtfertigen sollen.

Denn nach Klausel 5 b) des Beschlusses 2010/87/EU muss der drittstaatliche Auftragsverarbeiter garantieren, dass er seines Wissens nach keinen Gesetzen unterliegt, die ihm die Befolgung der anderen Klauseln unmöglich machen. Andernfalls ist der Verantwortliche berechtigt, seine grenzüberschreitende Datenverarbeitung auszusetzen. Eine Ausnahme gilt jedoch für drittstaatliches Recht, das nicht über das hinausgeht, was in einer demokratischen Gesellschaft für den Schutz eines der in Art. 23 Abs. 1 DSGVO (ehemals Art. 13 Abs. 1 DSRL) aufgelisteten Interessen wie der nationalen Sicherheit erforderlich ist (Fußnote 2 zu Klausel 5). Hieran sind die Zugriffsbefugnisse von NSA & Co. zu messen. Sie könnten sich als Achillesferse für sämtliche Informationsübermittlungen in die USA erweisen.

Die Presidential Policy Directive 28: Ein defizitärer Betroffenenschutz

Die zentralen Rechtsgrundlagen für die Auslandsaufklärung US-amerikanischer Sicherheitsbehörden sind *§ 702 Foreign Intelligence Surveillance Act* und die *Executive Order 12333*. Die Analyse des Generalanwalts zeigt: Effektiven Rechtsschutz bieten sie Unionsbürgern nicht (Rn. 254 ff.). Diesen verspricht allein die *Presidential Policy Directive 28* (PPD-28). Sie sollte die rechtliche Benachteiligung von Ausländern gegenüber US-Amerikanern in Datenschutzfragen überwinden (§ 4 PPD-28) und der massenhaften Datenausspähung Grenzen setzen (§ 2 PPD-28). Doch ihr Versprechen trügt.

Die Direktive hat weder Gesetzeskraft noch begründet sie individuelle Rechtsansprüche für Unionsbürger. Auch das Ende der Massenüberwachung hat sie nicht eingeläutet, findet sich in ihr doch eine folgenschwere Ausnahme für lediglich „temporär“ gespeicherte Daten (Fußnote 5 zur PPD-28). Zu Recht äußert der Generalanwalt daher erhebliche Zweifel daran, dass die Zugriffsrechte der US-Behörden mit der Feststellung eines angemessenen Datenschutzniveaus zu vereinbaren seien (Rn. 308). Die bestehenden Defizite ließen sich zudem nicht allein mit dem Schutzgut nationaler Sicherheit rechtfertigen (vgl. Rn. 306).

Ein Mehr an Betroffenenschutz kann auch die im Privacy Shield angelegte Ombudsperson nicht sicherstellen (vgl. Rn. 335). Zum einen verfügt sie über keine ausreichende Unabhängigkeit gegenüber der Exekutive, da ihr Amt mit dem eines Unterstaatssekretärs im US-Außenministerium verbunden ist. Zum anderen ist sie

nicht befugt, Unionsbürger überhaupt darüber zu informieren, ob sie überwacht worden sind oder nicht (vgl. ErwGr. 121 S. 2 Privacy Shield).

Das Fazit: Es kommt darauf an…

Die mitgliedstaatlichen Datenschutz-Aufsichtsbehörden mögen zwar nicht durch den Privacy Shield gebunden sein, wenn sie einzelne Datentransfers bewerten, die sich auf SCC stützen. Doch sollte sich der EuGH der Analyse des Generalanwalts anschließen und zu dem Ergebnis kommen, dass der Angemessenheitsbeschluss die Art. 7, Art. 8 und Art. 47 GRCh verletzt, könnten die Aufsichtsstellen dies nicht ignorieren.

Ob sich die Informationsübermittlung in die USA dann generell als unvereinbar mit dem Unionsrecht erwiese, wäre daran gekoppelt, ob die US-amerikanischen Vertragspartner der europäischen Unternehmen, die SCC nutzen, den dortigen Gesetzen zur Auslandsaufklärung unterliegen. So bindet etwa § 702 FISA alle *electronic communication service provider* (50 U.S.C. § 1881a [h] [2] [A] [vi]).

Besteht eine solche „Einbindung“ in die US-amerikanische Auslandsaufklärung hingegen nicht, könnten SCC sehr wohl auch über ein mögliches Ende des Privacy Shield hinaus grenzüberschreitende Datentransfers in die USA legitimieren. Es wären jedoch – sollte der EuGH auch diesbezüglich dem Generalanwalt folgen – die verschärften Handlungspflichten der Verantwortlichen zu berücksichtigen. SCC sind daher im Vergleich zu Angemessenheitsbeschlüssen mit weit mehr Aufsichts- und Kontrollmaßnahmen verbunden (vgl. Art. 45 Abs. 1 S. 2 DSGVO). Eine entscheidende Rolle haben in diesem System zudem die nationalen Datenschutzbehörden inne. Von ihrer Prüfungs- und Vollzugsdichte hängt ab, ob die SCC tatsächlich ein angemessenes i.S.v. gleichwertiges Schutzniveau bieten können. Ist dies nicht gewährleistet, herrscht auch weiterhin nur gesicherte Unsicherheit im transatlantischen Datenverkehr.
